Reference 1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-154233
(43)Date of publication of application : 27.05.1992

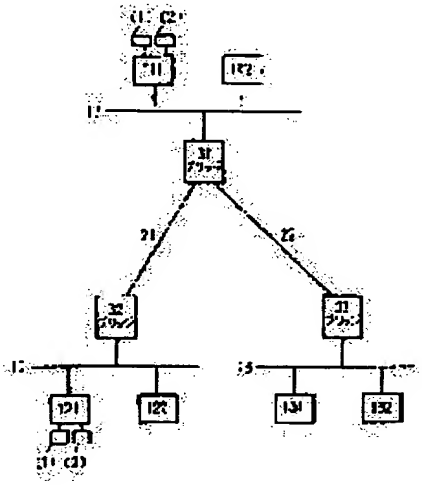
(51)Int.Cl. H04L 9/00
H04L 9/10
H04L 9/12
H04L 12/40

(21)Application number : 02-278216
(22)Date of filing : 17.10.1990

(71)Applicant : FUJITSU LTD
(72)Inventor : FUKUDA HARUKI

(54) COMMUNICATION CONCEALING METHOD

(57)Abstract:
PURPOSE: To make an unauthorized person difficult to read classified communication and further to carry out accurate communication between terminals by dividing the whole body of a cipher system into a cipher system of communication apparatuses in a network such as bridge, router, or the like and into a cipher system between terminals and by using the inter-terminal cipher system and the intra-network cipher system separately.
CONSTITUTION: A sending terminal 111 uses an inter-terminal cipher system 1 for dealing with information necessary to communicate with a party terminal 121 and an intra-network cipher system 2 for dealing with information necessary to carry out data transfer processing or the like in networks 11 and 12 or bridges 31 and 32. A party terminal 121 belonging to a network 12 uses the intra-network cipher system 2 to interprete part of the network of the message received from bridge 32, recognizes that the message is sent to the party terminal 121 itself, and uses the inter-terminal cipher system 1 to interprete inter-terminal information. With this, message communication between terminals 111 and 121 via networks 11 and 12 including bridges 31 and 32 or router is enciphered, thereby making an unauthorized person through networks 11 and 12 difficult to read the message communication and making it possible to carry out normal communication between terminals 111 and 121.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

Reference 1

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−154233

⑤1Int. Cl.⁵　識別記号　庁内整理番号　⑬公開　平成4年(1992)5月27日

H 04 L 9/00
9/10
9/12
12/40

7117−5K　H 04 L 9/00　Z
7928−5K　11/00　320

審査請求　未請求　請求項の数 2　(全5頁)

⑤4発明の名称　通信秘匿方式

⑳特　願　平2−278216
㉒出　願　平2(1990)10月17日

⑦2発明者　福田　治樹　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
⑦1出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
⑦4代理人　弁理士　井桁　貞一

明細書

1. 発明の名称

通信秘匿方式

2. 特許請求の範囲

1. ネットワークを介してメッセージ通信を行う端末が，送信する情報を暗号化して送出し，受信した情報を復号化する通信秘匿方式において、

各端末が端末相互間の暗号系(1)とネットワーク内の暗号系(2)の2種類の暗号系を具え、

端末間でのみ必要な情報には該端末相互間の暗号系(1)を使用し，ネットワークでの転送処理等に必要な情報には該ネットワーク内の暗号系(2)を使用することを特徴とした通信秘匿方式。

2. ネットワークを介してメッセージ通信を行う端末が，送信する情報を暗号化して送出し，受信した情報を復号化する通信秘匿方式において、

端末とネットワーク装置間の暗号系とネットワーク装置相互間の暗号系とを別にし、ネットワーク装置は端末からのネットワークでの転送処理等に使用する情報を第1の暗号系で解読し、ネットワーク装置相互間の第2の暗号系に変換して転送することを特徴とした通信秘匿方式。

3. 発明の詳細な説明

〔概要〕

ネットワークを介してメッセージ通信を行う端末が，送信する情報を暗号化して送出し，受信した情報を復号化する通信秘匿方式に関し、

ブリッジやルータを含むネットワークを介して行う端末間のメッセージ通信を暗号化しネットワークでの第三者の解読を困難にし当該端末間では正常通信を行なえる通信秘匿方式を目的とし、

端末が端末相互間の暗号系とネットワーク内の暗号系の2種類の暗号系を具え、端末間でのみ必要な情報には該端末相互間の暗号系を使用し，ネットワークでの転送処理等に必要な情報には該ネットワーク内の暗号系を使用するように構成する。また、端末とネットワーク装置間の暗号系とネッ

トワーク装置相互間の暗号系とを別にし、ネットワーク装置は端末からのネットワークでの転送処理等に使用する情報を第1の暗号系で解読し、ネットワーク装置相互間の第2の暗号系に変換して転送するように構成する。

〔産業上の利用分野〕

本発明は、ネットワークを介して端末間で行うメッセージ通信を、暗号化して秘匿する通信秘匿方式に関する。

IEEE 標準の CSMA/CD (Carrier Sense Multiple Access / Collision Detection) の LAN (Local Area Network) のように、端末間でメッセージ通信を行うネットワークでは、送受信アドレスと通信情報とが一つのメッセージとして送受信されるが、これを全て暗号化してしまうと、方式の異なる LAN間を接続するブリッジやルータを経由して通信する場合、該ブリッジやルータが転送すべきネットワークを正しく認識することが出来ず、正常な通信ができない。ネットワークで使用する部分のメッセージを暗号化しないと、通信した事と相手が誰かなどの情報が公開された状態となり、特定通信を傍受しようとする者にとっては、暗号化した情報を容易に入手することが可能となり解読を容易にする結果となる。

〔従来の技術〕

従来は、端末間のメッセージ通信の暗号化の場合、一般にネットワーク内の部分は暗号化せず、特にネットワーク内の部分を暗号化する場合は、ネットワーク通信の機器相互間の情報を暗号化していた。

〔発明が解決しようとする課題〕

したがって、CSMA/CD のLAN のように各端末がバス上の情報を自由に取り込めるようなネットワークでは、その端末寄りの部分では、通信の内容が秘匿されないという問題点があった。本発明の課題は、ブリッジやルータを含むネットワークを介して行う端末間のメッセージ通信を暗号化しネットワークでの第三者の解読を困難にして、当該端末間では正常通信を行なえる通信秘匿方式の提供にある。

〔課題を解決するための手段〕

この課題は、第1図の原理図の如く、複数のブリッジ(31,32,33)で接続される複数ネットワーク(11,12,13)に属する複数端末のなかの特定端末(111,121)間で行うメッセージ通信を暗号化して秘匿する通信秘匿方式において、各端末が端末相互間の暗号系(1) とネットワーク内の暗号系(2) の2種類の暗号系を具え、特定端末(111,121)間でのみ必要な情報には該端末相互間の暗号系(1) を使用し，ネットワーク(11,12)での転送処理等に必要な情報には該ネットワーク内の暗号系(2) を使用するように構成した本発明の第1発明の通信秘匿方式によって達成される。

又、この課題は、図示しないが、端末とネットワーク装置間の暗号系とネットワーク装置相互間の暗号系とを別にし、ネットワーク装置は端末からのネットワークでの転送処理等に使用する情報を第1の暗号系で解読し、ネットワーク装置相互間の第2の暗号系に変換して転送するように構成した本発明の第2発明によっても達成される。

〔作用〕

本発明の第1発明の通信秘匿方式は、第1図を参照し、送信端末111 は相手端末121 との通信に必要な情報のみには、端末相互間の暗号系(1) を適用し、ネットワーク11，12やブリッジ31,32での転送処理等に必要な情報には，ネットワーク内の暗号系(2) を適用する。 即ち、送信端末111は、自分の属するネットワーク11と相手端末121の属するネットワーク12とを接続するブリッジ31,32 のネットワークのアドレス等のネットワーク内のみで使用する情報には該ネットワーク内の暗号系(2) により暗号化し、両端末(111,121) 相互間のみの情報には該端末相互間の暗号系(1) で暗号化し、一つのメッセージとして自分111の属するネットワーク11へ送出する。そしてネットワー

ク11に接続されたブリッジ31は該メッセージを受信し該ネットワーク11で使用する部分を解読し、相手端末121 の属するネットワーク12と接続されるブリッジ32へ転送する。ブリッジ32も、同様にネットワーク12で使用する部分を解読し、該ネットワークへ該メッセージを送出する。ネットワーク12に属する相手端末121 は、ブリッジ32から受信したメッセージの中のネットワークで使用する部分をネットワーク内の暗号系(2) で解読し、自分宛であることを認識して端末間の情報を、端末相互間の暗号系(1) で解読する。

また、本発明の第2発明の通信秘匿方式は、図示しないが、端末とネットワーク装置間の暗号系とネットワーク装置相互間の暗号系とが別なので、ネットワーク装置は、端末からのネットワークでの転送処理等に使用する情報を、第1の暗号系で解読し、ネットワーク装置相互間の第2の暗号系に変換したのち、相手のネットワーク装置へ転送する。

等の情報に選別し、それぞれ、端末間暗号系1 とネットワーク内暗号系2 により、復号化する。そして、それら2系の復号化出力をセレクタSEL₂で選択し、受信データとして外部へ出力する。

第4図は本発明の第2発明の実施例の通信秘匿方式の構成を示すブロック図であり、全体の暗号系を、端末とネットワーク装置間の第1暗号系Aとネットワーク装置相互間の第2暗号系B とに別け、第1のネットワーク装置41は端末141からの該ネットワーク14での転送処理等に使用する情報を第1暗号系A で解読し、その暗号変換器A/B でネットワーク装置相互間の第2暗号系B に変換して第2のネットワーク装置42へ転送する。そして相手端末151 は、そのネットワーク装置42からの第2 暗号系B で暗号化された転送信号を、該装置42内の、前と逆の暗号変換器B/A で変換した第1暗号系A で解読して、自分宛であることを認識して端末141 と正常に通信する。

〔発明の効果〕

〔実施例〕

第2図のa,b は、本発明の第1発明の実施例の通信秘匿方式の送信端末と受信端末の各構成を示すブロック図であり、第3図は第1発明の実施例の動作を説明するための端局からネットワークへの送信信号のフレーム構成例を示す。

第2図のaの送信端末は、外部からの送信データを、セレクタSEL₁で、端末間のみで必要なデータや CRC信号等の情報と，ネットワーク内のみで必要な受信先アドレス，送信元アドレス等の情報とに選別し、それぞれ、端末間暗号系1 とネットワーク内暗号系2 により、暗号化する。そして、それら2系の暗号化出力を、セレクタSEL₂で選択し、第3図の構成例の如く、フレームを構成し、送信部によりネットワークへ送出する。

第2図のbの受信端末は、ネットワークからの第3図の如くフレーム構成された暗号化情報を、受信部で受信し、セレクタSEL₁で、端末間のみで必要なデータ,CRC信号等の情報と，ネットワーク内のみで必要な受信先アドレス，送信元アドレス

以上説明した如く、本発明によれば、CSMA/CDのLAN の様にメッセージ通信を行うネットワークで、全体の暗号系をブリッジ，ルータ等のネットワーク内の通信機器との暗号系と、端末相互間の暗号系とに分離し、端末間でのみ必要な情報には端末相互間の暗号系を使用し、ネットワークでの転送処理等に使用する情報にはネットワーク内の暗号系を使用するので、第三者の解読を困難とし当該端末間では正常な通信を行える効果が得られる。

4.図面の簡単な説明

第1図は本発明の第1発明の通信秘匿方式の基本構成を示す原理図、

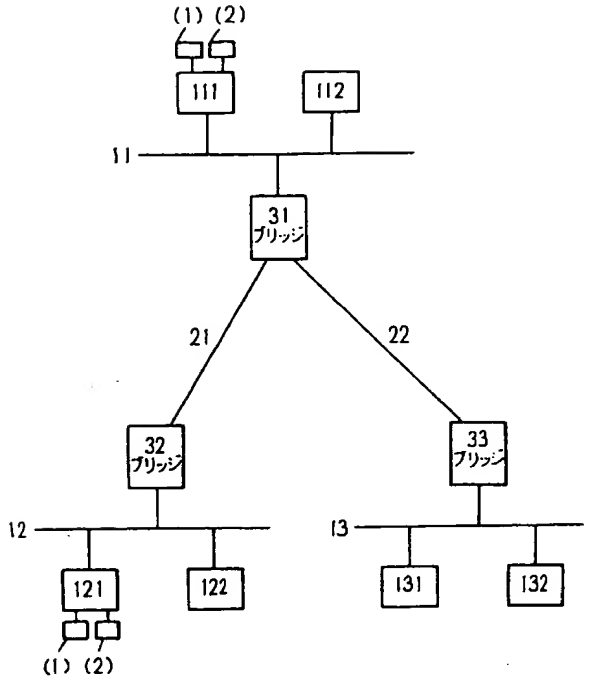
第2図は本発明の第1発明の実施例の通信秘匿方式のブロック図、

第3図は第1発明の実施例の動作を説明するための端局の送信信号のフレーム構成例を示す図、

第4図は本発明の第2発明の通信秘匿方式のブロック図である。

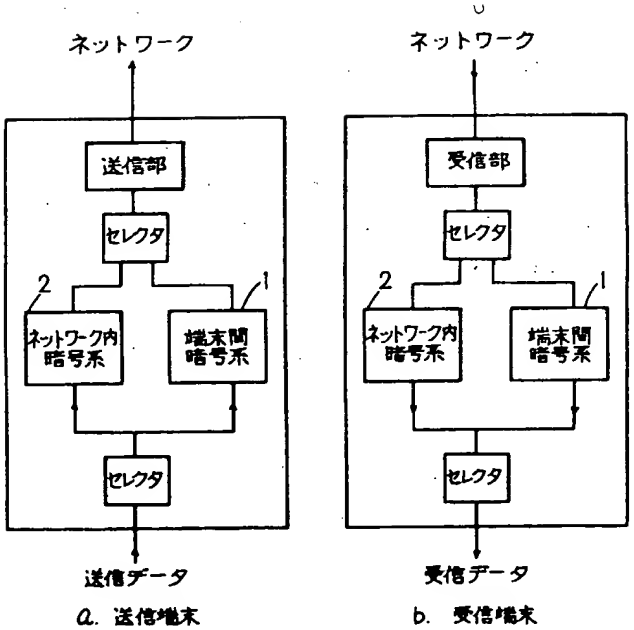
図において、1は端末相互間の暗号系、2はネットワーク内の暗号系、11,12,13,14,15はネットワーク、21,22は通信パス、31,32,33,41,42はブリッジ等のネットワーク機器、111,112,121,122,131,132,141,151は端末である。

代理人　弁理士　井桁貞一



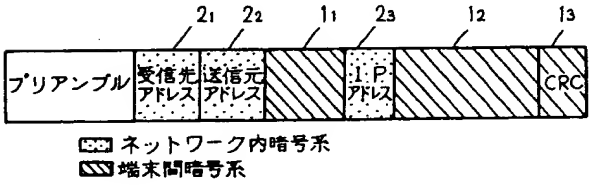
本発明の第1発明の通信秘匿方式の基本構成を示す原理図

第　1　図



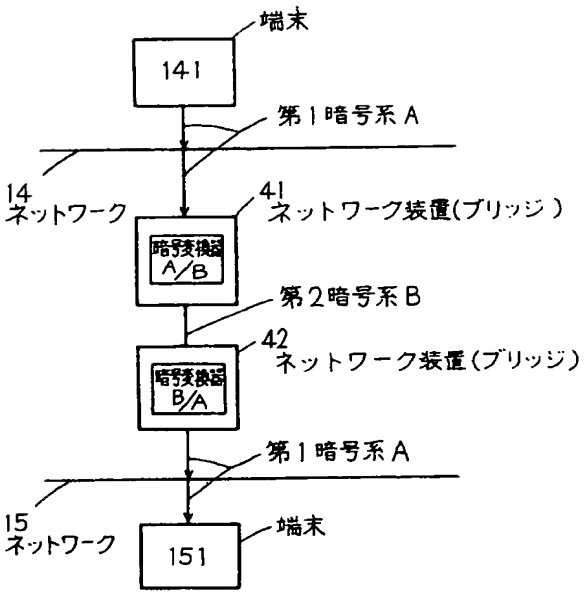
第1発明の実施例の送信端末と受信端末の構成を示すブロック図

第　2　図



第1発明の実施例の動作を説明するための端末の送信信号のフレーム構成例を示す図

第　3　図



本発明の第2発明の実施例の通信秘匿方式のブロック図

第 4 図